CHAPTER I: FINITE FIELDS
§3: QUADRATIC RECIPROCITY LAW

ALLEN LIN

1. Squares in $\mathbb{F}_q$

Quadratic reciprocity is one of the most remarkable and beautiful theorems in math. It is useful in determining the primes p such that n is a square modulo p.

Recall that order of a finite field is a power of a prime. Recall the characterisitic of a field K, denoted by $\text{char}(K)$, is the smallest integer $n > 0$ such that $n \cdot 1 = 0$. The characteristic of a field is prime.

We now start the study of squares in finite fields. There are two categories of primes: $p = 2$ and $p > 2$. When $p = 2$, we can classify all squares: all elements of $\mathbb{F}_q$ are perfect squares.

Theorem 1. *Let $p = 2$ and let q be a power of p. All elements of $\mathbb{F}_q$ are squares.*

Proof 1. There is one easy way to see this. Write $q = p^k$ for some $k \in \mathbb{N}$. If $a \in \mathbb{F}_q$, then consider the element $a^{2^{k-1}}$. Then a straightforward calculation shows that

$$\left(a^{2^{k-1}}\right)^2 = a^{2^k} = a^q = a,$$

as required. □

Proof 2. Another way of seeing this is noting that the map $\sigma\colon \mathbb{F}_q \to \mathbb{F}_q$ given by $\sigma(x) = x^2$ is an automorphism. We verify the axioms below. Recall that $\text{char}(\mathbb{F}_q) = 2$.

(1) By commutativity, $\sigma(xy) = (xy)^2 = x^2y^2 = \sigma(x)\sigma(y)$.
(2) Noting $\text{char}(\mathbb{F}_q) = 2$,
$$\sigma(x + y) = (x + y)^2 = x^2 + 2xy + y^2 = x^2 + y^2 = \sigma(x) + \sigma(y).$$
(3) Note $\sigma(1) = 1$ and $\sigma(0) = 0$.
(4) Note $\ker(\sigma)$ is an ideal of $\mathbb{F}_q$ and $\sigma \neq 0$, so $\ker(\sigma) = \{0\}$. Hence σ is injective.
(5) An injective map from a finite field to itself is surjective.

Hence σ is an automorphism. □

Now that we have classified all squares when $p = 2$, we consider when $p \neq 2$.

Theorem 2. *Let $p \neq 2$ and let q be a power of p. The squares of $\mathbb{F}_q^*$ is the kernel of the map $x \mapsto x^{(q-1)/2}$ and is a subgroup of index 2 in $\mathbb{F}_q^*$.*

The intuition in this theorem is that $\mathbb{F}_q^*$ can be partitioned into the quadratic residues and nonquadratic residues, and the two partitions are of equal size.

Proof. We need to determine when $x \in \mathbb{F}_q^*$ is a square. Let $\overline{\mathbb{F}_q^*}$ be the algebraic closure of $\mathbb{F}_q^*$ and let $y \in \overline{\mathbb{F}_q^*}$ such that $y^2 = x$. Thus, x is a square if and only if $y \in \mathbb{F}_q^*$. But $y \in \mathbb{F}_q^*$ if and only if $y^{q-1} = 1$. Consider the map $\sigma \colon \mathbb{F}_q^* \to \mathbb{F}_q^*$ given by $\sigma(x) = x^{(q-1)/2}$. Because $x^{q-1} = 1$, we have

$$y^{q-1} = \sigma\left(y^2\right) = \sigma(x) = x^{(q-1)/2} = \pm 1.$$

Thus, σ takes on 1 or -1 for all $x \in \mathbb{F}_q^*$. This means that x is a square if and only if $\sigma(x) = 1$, or equivalently that $x \in \ker(\sigma)$. Therefore, $\ker(\sigma) = (\mathbb{F}_q^*)^2$. Finally, $\mathbb{F}_q^*$ is cyclic of order $q-1$, so $\left(\mathbb{F}_q^*\right)^2$ has order $(q-1)/2$. □

2. Legendre Symbol

Our map $x \mapsto x^{(q-1)/2}$ motivates the definition of the Legendre symbol, which is useful in denoting elements that are squares. Recall that we are studying $p \neq 2$.

Definition 1. Let $p \neq 2$ and let $x \in \mathbb{F}_p^*$. The *Legendre symbol* of x is denoted by $\left(\frac{x}{p}\right) = x^{(p-1)/2} = \pm 1$.

This definition essentially asks whether x is a square in $\mathbb{F}_p$; if so, the symbol is 1 and otherwise -1. Naturally we define $\left(\frac{0}{p}\right) = 0$. We have the multiplicative property

$$\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = x^{(p-1)/2} y^{(p-1)/2} = (xy)^{(p-1)/2} = \left(\frac{xy}{p}\right).$$

This definition allows us to calculuate Legendre symbols for basic values of x. For example,

$$\left(\frac{1}{p}\right) = 1^{(p-1)/2} = 1,$$

so 1 is a square in $\mathbb{F}_p$. In fact, $1 = 1^2$. Moreover,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We can verify this formula directly. The Legendre symbol is -1 is $(p-1)/2$ is odd, or $(p-1)/2 = 2k+1$ for some $k \in \mathbb{Z}$; hence $p = 4k+3$. Conversely, the Legendre symbol is 1 if $(p-1)/2$ is even, or $(p-1)/2 = 2k$ for some $k \in \mathbb{Z}$; hence $p = 4k+1$.

Lemma 1. *We have*

$$\left(\frac{2}{p}\right) = 2^{(p-1)/2} = (-1)^{\left(p^2-1\right)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 5 \pmod 8. \end{cases}$$

Proof. Let α be an 8th primitive root in the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. Hence $\alpha^4 = -1$, so $\alpha^2 = -\alpha^{-2}$. Consider the element $y = \alpha + \alpha^{-1}$. Then $y^2 = 2 + \alpha^2 + \alpha^{-2} = 2$.

Moreover, since $\mathrm{char}(\mathbb{F}_p) = p$, it follows that $y^p = \alpha^p + \alpha^{-p}$. We now analyze the two cases separately. If $p \equiv \pm 1 \pmod 8$, then by symmetry $y^p = \alpha + \alpha^{-1} = y$, so

$$1 = y^{p-1} = \left(y^2\right)^{(p-1)/2} = 2^{(p-1)/2} = \left(\frac{2}{p}\right).$$

On the other hand, if $p \equiv \pm 5 \pmod 8$, then $y^p = \alpha^5 + \alpha^{-5} = \alpha^4\left(\alpha + \alpha^{-9}\right)$ by symmetry. Working modulo 8 this becomes $-\left(\alpha + \alpha^{-1}\right) = -y$, so

$$-1 = y^{p-1} = \left(y^2\right)^{(p-1)/2} = 2^{(p-1)/2} = \left(\frac{2}{p}\right).$$

The result follows. □

3. Quadratic Reciprocity Law

We now prove the famous result by Gauss. There are now at least 150 proofs of this result, but we will prove it using Guass sums.

Theorem 3. *Let l and p be distinct primes not 2. Then*

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

We prove this result through two lemmas. Again, let $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$, and let $w \in \overline{\mathbb{F}_p}$ be a lth primitive root of unity. Therefore, $w^l = 1$ and w^x is defined for all $x \in \mathbb{F}_l$. We consider the Gauss sum

$$y = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) w^x.$$

The first lemma gives us a result on the square of the Gauss sum.

Lemma 2. *We have $y^2 = (-1)^{(l-1)/2} l$.*

The second lemma relates the Gauss sum with the Legendre symbol.

Lemma 3. *We have $y^{p-1} = \left(\frac{p}{l}\right)$.*

These two lemma immediately imply the quadratic reciprocity law, as

$$\left(\frac{(-1)^{(l-1)/2} l}{p}\right) = \left(\frac{y^2}{p}\right) = \left(y^2\right)^{(p-1)/2} = y^{p-1} = \left(\frac{p}{l}\right)$$

by Lemma 2, but on the other hand

$$\left(\frac{(-1)^{(l-1)/2} l}{p}\right) = \left((-1)^{(l-1)/2} l\right)^{(p-1)/2} = \left(\frac{l}{p}\right)(-1)^{(l-1)(p-1)/4}$$

by Lemma 3. Equating these identities give the result.

Now we prove Lemma 2.

Proof of Lemma 2. Note

$$y^2 = \left(\sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right)w^x\right)\left(\sum_{z\in\mathbb{F}_l}\left(\frac{z}{l}\right)w^z\right) = \sum_{(x,z)\in\mathbb{F}_l^2}\left(\frac{xz}{l}\right)w^{x+z}.$$

With the change of variables $u = x + z$ and $t = x$, this becomes

$$y^2 = \sum_{u\in\mathbb{F}_l} w^u \sum_{t\in\mathbb{F}_l}\left(\frac{t(u-t)}{l}\right) = \sum_{u\in\mathbb{F}_l} w^u \sum_{t\in\mathbb{F}_l^*}\left(\frac{t(u-t)}{l}\right), \tag{1}$$

where in the last step we take out the $t = 0$ term in the inner sum. Now $t \neq 0$ in $\mathbb{F}_l^*$, so $t^{-1} \in \mathbb{F}_l^*$ and

$$\left(\frac{t(u-t)}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right) = (-1)^{(l-1)/2}\left(\frac{1-ut^{-1}}{l}\right).$$

Set

$$C(u) \coloneqq \sum_{l\in\mathbb{F}_l^*}\left(\frac{1-ut^{-1}}{l}\right).$$

Note that if $u = 0$, then $C(0) = l-1$. Moreover, ut^{-1} runs over the elements of $\mathbb{F}_l\setminus\{0\}$ as u ranges from $\mathbb{F}_l \setminus \{0\}$, so in the same range $1 - ut^{-1}$ runs over the elements of $\mathbb{F}_l \setminus \{1\}$. Hence for $u \neq 0$ we have

$$C(u) = \sum_{s\in\mathbb{F}_l\setminus\{1\}}\left(\frac{s}{l}\right) = \sum_{s\in\mathbb{F}_l}\left(\frac{s}{l}\right) - \left(\frac{1}{l}\right) = -\left(\frac{1}{l}\right) = -1,$$

since in $\mathbb{F}_q$ the size of the partitions of squares and nonsquares are equal by Theorem 2. Thus, (1) becomes

$$y^2(-1)^{(l-1)/2} = \sum_{u\in\mathbb{F}_l} w^u C(u) = l - 1 + \sum_{u\in\mathbb{F}_l\setminus\{0\}} w^u C(u) = l - 1 - \sum_{u\in\mathbb{F}_l\setminus\{0\}} w^u = l, \tag{2}$$

noting that

$$\sum_{u\in\mathbb{F}_l\setminus\{0\}} w^u = -1.$$

Hence (2) implies our result $y^2 = (-1)^{(l-1)/2}l$. □

Now we prove Lemma 3.

Proof of Lemma 3. Because $\overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$, we have $\mathrm{char}(\overline{\mathbb{F}_p}) = p$ and

$$y^p = \sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right)^p w^{xp} = \sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right)w^{xp}.$$

With the change of variables $z = xp$ this becomes

$$y^p = \sum_{z\in\mathbb{F}_l}\left(\frac{zp^{-1}}{l}\right)w^z = \left(\frac{p^{-1}}{l}\right)\sum_{z\in\mathbb{F}_l}\left(\frac{z}{l}\right)w^z = \left(\frac{p}{l}\right)y,$$

noting

$$\left(\frac{p^{-1}}{l}\right) = \left(\frac{p}{l}\right)^{-1} = \left(\frac{p}{l}\right).$$

Hence $y^{p-1} = \left(\frac{p}{l}\right)$. □

Massachusetts Institute of Technology, 77 Massachusetts Ave, Cambridge, MA 02139-4301

Email address: allenees@mit.edu